/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/489,192	01/20/2000	SCOTT A. FIELD	MSI-407US	5535

22801 7590 06/18/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER
PARTHASARATHY, PRAMILA

ART UNIT	PAPER NUMBER
2136	9

DATE MAILED: 06/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/489,192	**Applicant(s)** FIELD, SCOTT A.
	Examiner Pramila Parthasarathy	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _03/24/2004_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-48_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-48_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment, Paper No. 7, filled on March 24, 2004. No claims have been cancelled or added. Claim 30 has been amended. Presently pending claims are 1 – 48.

Response to Argument

2. Applicant's argument filled on March 24, 2004, Paper No. 7 has been fully considered but they are not persuasive for the following reasons:

The applicant in regard to claims 1 – 29 and 36 – 48 argue that the cited prior art [Herbert et al. (5,757,919), Bryant et al. (5,628,023), and Buer et al. (6,003,117)] does not teach that "a key that is page-locked in the physical (main) memory", "page-lock the key" or store the key in a non-pageable page". These arguments are not found persuasive. Herbert describes and teaches that a key is generated at the encryption/decryption engine 12, which encrypts the pages before paging out the encrypted information and that the encryption/decryption engine is within the secure environment (Fig. 3; Column 1 Line 53 – Column 2 line 3 and Column 2 lines 25 – 69).. The key is stored and retrieved from the storage at functional block 62 (Fig. 3 #120, 124, 125; Column 7 lines 7 – 12 and 26 – 29). Herbert also discloses that the page containing key information is retained in the secure memory (Column 1 lines 35 – 40 and Column 5 lines 26 – 40).

Therefore, the examiner respectfully asserts that the cited prior art does teach or suggest the subject matter "a key that is page-locked in the physical memory", "page-lock the key", and "store the key in a non-pageable page" broadly recited in the independent claims 1, 11, 19, 25, 36, 41, 42, 47 and 48. The dependent claims 2 – 10, 12 – 18, 26 – 29, 37 – 40 and 43 – 46 are rejected at least by virtue of their dependency on the independent claims and by other reason set forth in the previous office action (Paper No. 7).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-10, and 25 - 48 are rejected under 35 U.S.C. 102(b) as being anticipated by Herbert et al. (US Patent No. 5,757,919).

As per claim 1, Herbert teaches a method for encrypting information using a key in the physical memory and paging out the encrypted information (Col. 1 Lines 65 – 67 and Col. 2 Lines 2 – 3).

As per claim 2, Herbert teaches a method for encrypting, creating the key and page locking the key in the physical memory (Col. 1 Lines 60 - 65).

As per claim 3, Herbert teaches a method for creating the key during system boot up (Col. 2 Lines 45 – 52).

As per claim 4, Herbert teaches a method for generating a random key with a random key generator (Col. 2 Line 67 and Col. 3 Lines 1-2).

As per claim 5, Herbert teaches using RSA RC4 encryption algorithm to generate the key (Col. 3 Lines 25 – 32).

As per claims 6 and 8, Herbert teaches a method for calling an operating system kernel and the kernel using the page-locked key to encrypt the information. Herbert also teaches to implement claim 6 by an operating system memory manager (Col. 2 Lines 47– 49).

As per claim 7, Herbert teaches the use of an application to implement claim 6 (Col. 3 Lines 13 – 15).

As per claim 9, Herbert teaches a method for implementing with computer-readable media having computer-readable instructions to implement claim 1 (Fig. 3).

As per claim 10, Herbert teaches an operating system programmed with instructions to implement the method of claim 1 (Col. 5 Lines 59 – 67).

As per claim 25, Herbert teaches allocating a non-pageable page of main memory (Col.1 60-62); generating a random key (Col. 2 Line 67 and Col. 3 Lines 1-2); storing the random key in the non-pageable page of main memory; the operating system to encrypt information that might be paged out to the page file (Col.2 Lines 2-3).

As per claim 26, Herbert teaches using RSA RC4 encryption algorithm to generate the key (Col. 3 Lines 25 – 32).

As per claim 27, Herbert teaches a method for creating the key during system boot up (Col. 2 Lines 45 – 52).

As per claim 28, Herbert teaches a method for implementing with computer-readable media having computer-readable instructions to implement claim 25 (Fig. 3).

As per claim 29, Herbert teaches an operating system programmed with instructions to implement the method of claim 25 (Col. 5 Lines 59 – 67).

As per Claim 30, Herbert teaches and describes an operating system having main memory for holding information and secondary storage for receiving information that is transferred out of main memory, a computer-implemented method of protecting information (Fig. 1 – 4a and Column 1 line 14 – Column 7 line 52) comprising:

generating at least one non-pageable random key by using a random key generation process (Fig. 3 #120; Column 1 lines 35 – 40; Column 2 line 39 – Column 3 and Column 5 lines 26 – 40);

encrypting at least one selected block of information in the main memory with a software component that uses the at least one random key for encryption (Fig. 3 #124 Column 4 lines 60 – 65 and Column 6 lines 31 – 65);

transferring the one encrypted block of information to the secondary storage (Fig. 3 # 125; Column 1 lines 35 – 40; Column 2 line 39 – Column 3 and Column 5 lines 26 – 40);

decrypting the one encrypted block of information with the software component that uses the at least one random key for decryption (Fig. 5b; Column 3 lines 2 – 8 and Column 7 lines 7 – 20); and

placing the decrypted block of information in the main memory (Fig.5b Column 7 lines 7 – 33).

Claim 31 is rejected as applied above in rejecting claim 30. Furthermore, Herbert teaches and describes an operating system having main memory for holding information and secondary storage for receiving information that is transferred out of main memory, a computer-implemented method of protecting information (Fig. 1 – 4a and Column 1 line 14 – Column 7 line 52) wherein said generating is performed during system boot up (Column 2 line 45 – Column 3 line 2).

Claim 32 is rejected as applied above in rejecting claim 30. Furthermore, Herbert teaches and describes an operating system having main memory for holding information and secondary storage for receiving information that is transferred out of main memory, a computer-implemented method of protecting information (Fig. 1 – 4a and Column 1 line 14 – Column 7 line 52) further comprising restricting access to the at least one random key to only the software component (Column 3 lines 9 – 15).

Claim 33 is rejected as applied above in rejecting claim 30. Furthermore, Herbert teaches and describes an operating system having main memory for holding information and secondary storage for receiving information that is transferred out of main memory, a computer-implemented method of protecting information (Fig. 1 – 4a and Column 1 line 14 – Column 7 line 52) wherein the software component comprises the operating system's kernel (Column 2 line 47 – Column 3 line 15).

Claim 34 is rejected as applied above in rejecting claim 30. Furthermore, Herbert teaches and describes an operating system having main memory for holding information and secondary storage for receiving information that is transferred out of main memory, a computer-implemented method of protecting information (Fig. 1 – 4a and Column 1 line 14 – Column 7 line 52) further comprising:

storing the at least one random key in the main memory (Fig.3 # 120; Column 1 lines 35 – 40; Column 2 line 64 – Column 3 line 2 and Column 5 lines 26 – 40); and locking the at least one random key in the main memory so that it does not get transferred to the second storage (Fig. 4a & b; Column 1 lines 35 – 40 and Column 5 lines 26 – 40).

Claim 35 is rejected as applied above in rejecting claim 30. Furthermore, Herbert teaches and describes an operating system programmed with instructions which, when implemented by the operating system (Column 2 line39 – Column 3 line 15), implemented the method of having main memory for holding information and secondary storage for receiving information that is transferred out of main memory, a computer-implemented method of protecting information (Fig. 1 – 4a and Column 1 line 14 – Column 7 line 52).

As per claim 36, Herbert teaches that a memory having pageable and non-pageable pages and key being configured for use in encrypting pageable information (Col. 5 Lines 26 – 29).

As per claim 37, Herbert teaches that this can easily be implemented as software (Col. 3 Lines 13-15).

As per claim 38, Herbert teaches that the key is accessible only to the software component (Col. 2 Lines 45 – 47).

As per claim 39, Herbert teaches that the application configured to call the software component to encrypt the pageable information (Col. 3 Lines 9 – 15).

As per claim 40, Herbert teaches to implement claim 37 by a memory manager (Col. 2 Lines 47– 49). Herbert also teaches the use of an application to implement claim 36 (Col. 3 Lines 13 – 15).

As per claim 41 and 42, Herbert teaches a computer program comprising a processor, main memory, secondary storage (Fig. 1) and

encrypting information with a key that is page-locked in main memory and paging out, to secondary storage, the encrypted information (Col. 1 Lines 65 – 67 and Col. 2 Lines 2 – 3); accessing the encrypted information in the secondary storage (Col. 4 Lines 43 – 44); decrypting the encrypted information with the key that is page-locked in the main memory (Col. 3 Lines 2 – 5).

As per claim 43 and 44, Herbert teaches that the program generates the key and locks the key in the main memory and the same key is used to decrypt the information (Col. 4 Lines 23-25).

As per claim 45, Herbert teaches the use of software component that is programmed to encrypt and decrypt the information 42 (Col. 3 Lines 13 – 15).

As per claim 46, Herbert teaches the computer-implemented method of claim 45 wherein the software component comprises the operating system kernel (Col. 2 Lines 47 – 53).

As per claim 47, Herbert teaches an application programming interface comprising an interface method for encrypting pageable information with a key that is page-locked in the main memory and an interface method for decrypting encrypted information that is contained in the page file (Col. 2 Lines 63 – 67).

As per claim 48, Herbert teaches an application programming interface comprising a method for setting an attribute on a page of main memory, the attribute designating that the page must be encrypted with a key that is page-locked in the main memory prior to the page being paged out to the page file (Col. 3 Lines 13 – 15 and Col.1 60 – 63).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 11-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herbert et al. (5, 757,919) in view of Bryant et al. (5,628,023).

As per claim 11, Herbert et al. discloses a method for page-locking a key in main memory; calling the operating system kernel to encrypt information; using the operating system kernel to encrypt the information with the page locked key (Col. 5 Lines 59 –

67). Herbert et al. does not disclose a method for restricting access to the page-locked key to only the operating system kernel. However, Bryant et al. discloses a method for restricting access to the page-locked key to the operating system kernel (Col. 9 Lines 64-67 and Col.10 Lines 1-4). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Herbert by including a method for restricting access to the page-locked key to the only the operating system kernel as taught by Bryant. Such modification would have been obvious because by restricting the access to the kernel the user or other applications cannot access the page-locked key thereby making the system more secure.

As for claim12, Bryant discloses a method for calling the operating system kernel to encrypt information by an operating system memory manager (Fig. 7a) as claimed by claim 11.

As for claim 13, Bryant discloses a method for calling the operating system kernel to encrypt information by an application (Fig. 7a) as claimed by claim 11.

As for claim 14, Bryant discloses a method for calling the operating system kernel to encrypt information by designating a page in the main memory with a designation (Col. 9 Lines 37 – 39) and recognizing the designation (Col. 9 Lines 64-67).

As for claim 15, Bryant discloses memory manager is often implemented as part of the operating system (Col. 8 Lines 41 – 46).

As for claim 16, Herbert teaches specifying memory location and a memory size associated with the information to be encrypted (Col.3 Lines 43 – 48).

As for claim 17, Bryant discloses a computer-readable media having computer-readable instructions thereon which, when executed by a computer, perform the computer-implemented method of claim 11 (Fig. 1)

As for claim 18, Bryant discloses an operating system programmed with instructions which when implemented by the operating system, implement the method of claim 11 (Col. 9 Lines 35 – 39).

4.1. Claims 19 - 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herbert et al. (5, 757,919) in view of Buer et al. (6,003,117).

As per claim 19, Herbert et al. discloses a method for accessing encrypted information in the page file (Col. 4 Lines 43 – 44). Herbert et al. does not disclose a method for decrypting the encrypted information with a key that is page-locked in the main memory. However, Buer et al. disclose a method for decrypting the encrypted information with a key that is page-locked in the main memory (Col. 2 Lines 27-36). Therefore, it would have been obvious to a person of ordinary skill in the art to modify Herbert by including a method for decrypting the encrypted information with a key that is page-locked in the main memory as taught by Buer to protect the key that is page-locked in the main memory thereby making the system more secure.

As per claim 20, Buer discloses placing the decrypted information in a page of main memory (Col. 2 Lines 1-2).

As per claim 21, Buer discloses placing the decrypted information in a page-locked page of main memory (Col. 1 Lines 19 - 23).

As per claim 22, Herbert teaches the computer-implemented method of claim 19 wherein the page locked key is accessible only to the operating system kernel (Col. 2 Lines 47 – 53).

As per claim 23, Herbert teaches a method for implementing with computer-readable media having computer-readable instructions to implement claim 19 (Fig. 3).

As per claim 24, Herbert teaches an operating system programmed with instructions to implement the method of claim 19 (Col. 5 Lines 59 – 67).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Draganoff (U.S. Patent Number: 5,541,988) "Telephone dialer with a personalized page organization of telephone directory memory"

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 **or**

faxed to: (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy
Patent Examiner
703-305-8912
June 08, 2004.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100